The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSD) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the NVD, which contains historical vulnerability information.

The vulnerabilities are based on the CVE vulnerability naming standard and are organized according to severity, determined by the Common Vulnerability Scoring System (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

## High Vulnerabilities

| Primary<br>Vendor -- Product | Description | Discovered<br>Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| 8pixel.net -- Simple Blog | SQL injection vulnerability in comments.asp in SimpleBlog 2.0 and earlier allows remote attackers to execute arbitrary SQL commands via the id parameter. | unknown<br>2006-08-22 | 7.0 | CVE-2006-4300<br>BUGTRAQ<br>OTHER-REF<br>OTHER-REF<br>BID<br>SECUNIA<br>XF |
| AK-Systems -- Windows Terminal | VNC server on the AK-Systems Windows Terminal 1.2.5 ExVLP is not password protected, which allows remote attackers to login and view RDP or Citrix sessions. | unknown<br>2006-08-23 | 10.0 | CVE-2006-4309<br>BUGTRAQ<br>BID |
| All Topics -- All Topics Hack | SQL injection vulnerability in alltopics.php in the All Topics Hack 1.5.0 and earlier for phpBB 2.0.21 allows remote attackers to execute arbitrary SQL commands via the start parameter. | unknown<br>2006-08-26 | 7.0 | CVE-2006-4367<br>OTHER-REF<br>BID |
| Alt-N -- WebAdmin | Alt-N WebAdmin 3.2.3 and 3.2.4 running with MDaemon 9.0.5, and possibly earlier, allow remote authenticated domain administrators to change a global administrator's password and gain privileges via the userlist.wdm file. | unknown<br>2006-08-26 | 7.0 | CVE-2006-4370<br>BUGTRAQ<br>FULLDISC<br>OTHER-REF<br>BID<br>FRSIRT<br>SECUNIA<br>XF |
| AOL -- AOL Security Edition | AOL 9.0 Security Edition revision 4184.2340, and probably other versions, uses insecure permissions (Everyone/Full Control) for the "America Online 9.0" directory, which allows local users to gain privileges by replacing critical files. | unknown<br>2006-08-21 | 7.0 | CVE-2006-0948<br>BID<br>BUGTRAQ<br>FRSIRT<br>SECTRACK<br>SECUNIA<br>XF |
| Arthur Konze WebDesign -- AkoComment | PHP remote file inclusion vulnerability in akocomments.php in AkoComment 1.1 module (com_akocomment) for Mambo 4.5 allows remote attackers to execute arbitrary PHP code via a URL in the mosConfig_absolute_path parameter. | unknown<br>2006-08-21 | 7.0 | CVE-2006-4281<br>BUGTRAQ<br>BID<br>XF |
| bits-dont-bite -- EstateAgent | PHP remote file inclusion vulnerability in estateagent.php in the EstateAgent component (com_estateagent) for Mambo, when register_globals is enabled, allows remote attackers to execute arbitrary PHP code via a URL in the mosConfig_absolute_path parameter. | unknown<br>2006-08-23 | 7.0 | CVE-2006-4322<br>BUGTRAQ<br>BID |
| CityForFree -- indexcity | SQL injection vulnerability in list.php in CityForFree indexcity 1.0, when magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary SQL commands via the cate_id parameter. | unknown<br>2006-08-23 | 7.0 | CVE-2006-4323<br>OTHER-REF<br>BID<br>SECUNIA |
| CityForFree -- indexcity | Cross-site scripting (XSS) vulnerability in add_url2.php in CityForFree indexcity 1.0 allows remote attackers to inject arbitrary web script or HTML via the url parameter. | unknown<br>2006-08-23 | 7.0 | CVE-2006-4324<br>OTHER-REF<br>BID<br>SECUNIA |

| | | | | |
|---|---|---|---|---|
| CloudNine -- Interactive Links Manager | Multiple cross-site scripting (XSS) vulnerabilities in add_url.php in CloudNine Interactive Links Manager 2006-06-12 allow remote attackers to inject arbitrary web script or HTML via the (1) title, (2) description, or (3) keywords parameters. | unknown<br>2006-08-23 | 7.0 | CVE-2006-4327<br>OTHER-REF<br>BID<br>SECUNIA |
| CloudNine -- Interactive Links Manager | SQL injection vulnerability in admin.php in CloudNine Interactive Links Manager 2006-06-12, when magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary SQL commands via the nick parameter. | unknown<br>2006-08-23 | 7.0 | CVE-2006-4328<br>OTHER-REF<br>BID<br>SECUNIA |
| Constructor component -- Constructor component | PHP remote file inclusion vulnerability in admin.lurm_constructor.php in the Lurm Constructor component (com_lurm_constructor) 0.6b and earlier for Mambo allows remote attackers to execute arbitrary PHP code via a URL in the lm_absolute_path parameter. | unknown<br>2006-08-26 | 7.0 | CVE-2006-4372<br>OTHER-REF<br>XF |
| Contacts XTD component -- Contacts XTD component | ** DISPUTED ** PHP remote file inclusion vulnerability in contxtd.class.php in the Contacts XTD (ContXTD) component for Mambo (com_contxtd) allows remote attackers to execute arbitrary PHP code via a URL in the mosConfig_absolute_path parameter. NOTE: another researcher has disputed this issue, saying that the software prevents the attack by checking whether _VALID_MOS is defined. | unknown<br>2006-08-26 | 7.0 | CVE-2006-4375<br>BUGTRAQ<br>BUGTRAQ |
| Coppermine -- Photo Gallery component | PHP remote file inclusion vulnerability in cpg.php in the Coppermine Photo Gallery component (com_cpg) 1.0 and earlier for Mambo allows remote attackers to execute arbitrary PHP code via a URL in the mosConfig_absolute_path parameter. | unknown<br>2006-08-23 | 7.0 | CVE-2006-4321<br>OTHER-REF<br>BID<br>FRSIRT<br>SECUNIA<br>XF |
| CropImage component -- CropImage component | PHP remote file inclusion vulnerability in admin.cropcanvas.php in the CropImage component (com_cropimage) 1.0 for Mambo allows remote attackers to execute arbitrary PHP code via a URL in the cropimagedir parameter. | unknown<br>2006-08-26 | 7.0 | CVE-2006-4363<br>BUGTRAQ<br>OTHER-REF<br>BID |
| CubeCart -- CubeCart | Multiple SQL injection vulnerabilities in CubeCart 3.0.11 and earlier allow remote attackers to execute arbitrary SQL commands via the (1) oid parameter in modules/gateway/Protx/confirmed.php and the (2) x_invoice_num parameter in modules/gateway/Authorize/confirmed.php. | unknown<br>2006-08-21 | 7.0 | CVE-2006-4267<br>BUGTRAQ<br>OTHER-REF<br>OTHER-REF<br>OTHER-REF<br>OTHER-REF<br>OTHER-REF<br>BID<br>FRSIRT<br>SECTRACK<br>SECUNIA<br>XF |
| CubeCart -- CubeCart | Multiple cross-site scripting (XSS) vulnerabilities in CubeCart 3.0.11 and earlier allow remote attackers to inject arbitrary web script or HTML via the (1) file, (2) x, and (3) y parameters in (a) admin/filemanager/preview.php; and the (4) email parameter in (b) admin/login.php. | unknown<br>2006-08-21 | 7.0 | CVE-2006-4268<br>BUGTRAQ<br>OTHER-REF<br>OTHER-REF<br>OTHER-REF<br>BID<br>FRSIRT<br>SECTRACK<br>SECUNIA<br>XF |
| Derek Leung -- pSlash | PHP remote file inclusion vulnerability in modules/visitors2/include/config.inc.php in pSlash 0.70 allows remote attackers to execute arbitrary PHP code via a URL in the lvc_include_dir parameter. | unknown<br>2006-08-26 | 7.0 | CVE-2006-4373<br>BUGTRAQ<br>OTHER-REF<br>BID |
| DieselScripts -- Diesel Smart Traffic | PHP remote file inclusion vulnerability in clients/index.php in Diesel Smart Traffic allows remote attackers to execute arbitrary PHP code via a URL in the src parameter. | unknown<br>2006-08-26 | 7.0 | CVE-2006-4357<br>BUGTRAQ<br>BID<br>XF |
| DieselScripts -- Diesel Pay | Cross-site scripting (XSS) vulnerability in index.php in Diesel Pay allows remote attackers to inject arbitrary web script or HTML via the read parameter. | unknown<br>2006-08-26 | 7.0 | CVE-2006-4358<br>BUGTRAQ<br>BID<br>FRSIRT<br>SECUNIA<br>XF |
| DieselScripts -- Diesel Job Site | Multiple cross-site scripting (XSS) vulnerabilities in jobseekers/forgot.php in Diesel Job Site allow remote attackers to inject arbitrary web script or HTML via the (1) uname or (2) SEmail parameters. | unknown<br>2006-08-26 | 7.0 | CVE-2006-4361<br>BUGTRAQ<br>FRSIRT<br>SECUNIA<br>XF |

| | | | | |
|---|---|---|---|---|
| DieselScripts -- Diesel Paid Mail | Cross-site scripting (XSS) vulnerability in getad.php in Diesel Paid Mail allows remote attackers to inject arbitrary web script or HTML via the ps parameter. | unknown<br>2006-08-26 | 7.0 | CVE-2006-4362<br>BUGTRAQ<br>BID<br>FRSIRT<br>SECUNIA<br>XF |
| Digium -- Asterisk | Stack-based buffer overflow in channels/chan_mgcp.c in MGCP in Asterisk 1.0 through 1.2.10 allows remote attackers to execute arbitrary code via a crafted audit endpoint (AUEP) response. | unknown<br>2006-08-24 | 7.0 | CVE-2006-4345<br>OTHER-REF<br>OTHER-REF<br>BID<br>SECTRACK |
| Digium -- Asterisk | Asterisk 1.2.10 supports the use of client-controlled variables to determine filenames in the Record function, which allows remote attackers to (1) execute code via format string specifiers or (2) overwrite files via directory traversals involving unspecified vectors, as demonstrated by the CALLERIDNAME variable. | unknown<br>2006-08-24 | 7.0 | CVE-2006-4346<br>OTHER-REF<br>BID<br>SECTRACK |
| Doika -- Doika guestbook | Cross-site scripting (XSS) vulnerability in gbook.php in Doika guestbook 2.5, and possibly earlier, allows remote attackers to inject arbitrary web script or HTML via the page parameter. | unknown<br>2006-08-23 | 7.0 | CVE-2006-4325<br>OTHER-REF<br>FRSIRT<br>SECUNIA |
| FreeBSD -- FreeBSD<br>NetBSD -- NetBSD | Buffer overflow in the ppp driver in FreeBSD 4.11 to 6.1 and NetBSD 2.0 through 4.0 beta allows remote attackers to cause a denial of service (panic), obtain sensitive information, and possibly execute arbitrary code via crafted Link Control Protocol (LCP) packets with an option length that exceeds the overall length, which triggers the overflow in (1) pppoe and (2) ippp. | unknown<br>2006-08-23 | 10.0 | CVE-2006-4304<br>FREEBSD<br>OTHER-REF<br>NETBSD |
| Fscripts -- Fantastic News | PHP remote file inclusion vulnerability in news.php in Fantastic News 2.1.3 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the CONFIG[script_path] parameter. | unknown<br>2006-08-22 | 7.0 | CVE-2006-4285<br>OTHER-REF<br>OTHER-REF<br>BID<br>SECUNIA<br>FRSIRT<br>XF |
| Fusionphp -- Fusion News | PHP remote file inclusion vulnerability in index.php in Fusion News 3.7 allows remote attackers to execute arbitrary PHP code via a URL in the fpath parameter. | unknown<br>2006-08-21 | 7.0 | CVE-2006-4240<br>BUGTRAQ<br>BID<br>FRSIRT<br>SECTRACK<br>XF |
| Guder und Koch Netzwerktechnik -- Eichhorn Portal | Multiple cross-site scripting (XSS) vulnerabilities in Guder und Koch Netzwerktechnik Eichhorn Portal allow remote attackers to inject arbitrary web script or HTML via unspecified vectors, possibly including the (1) profil_nr and (2) sprache parameters in the main portion of the portal, the (3) suchstring field in suchForm in the main portion of the portal, the (4) GaleryKey and (5) Breadcrumbs parameters in the gallerie module, and the (6) GGBNSaction parameter in the ggbns module. | unknown<br>2006-08-26 | 7.0 | CVE-2006-4376<br>BUGTRAQ<br>XF |
| Guder und Koch Netzwerktechnik -- Eichhorn Portal | Multiple SQL injection vulnerabilities in Guder und Koch Netzwerktechnik Eichhorn Portal allow remote attackers to execute arbitrary SQL commands via unspecified vectors, possibly including the (1) profil_nr and (2) sprache parameters in the main portion of the portal, the (3) suchstring field in suchForm in the main portion of the portal, the (4) GaleryKey and (5) Breadcrumbs parameters in the gallerie module, and the (6) GGBNSaction parameter in the ggbns module. | unknown<br>2006-08-26 | 7.0 | CVE-2006-4377<br>BUGTRAQ<br>XF |
| IBM -- AIX | Unspecified vulnerability in setlocale in IBM AIX 5.1.0 through 5.3.0 allows local users to gain privileges via unspecified vectors. | unknown<br>2006-08-21 | 7.0 | CVE-2006-4254<br>OTHER-REF<br>AIXAPAR<br>AIXAPAR<br>AIXAPAR<br>BID<br>SECTRACK<br>SECUNIA<br>FRSIRT<br>OSVDB<br>XF |
| IntegraMOD -- IntegraMOD Portal | PHP remote file inclusion vulnerability in includes/functions_portal.php in IntegraMOD Portal 2.x and earlier allows remote attackers to execute arbitrary PHP code via a URL in the phpbb_root_path parameter. | unknown<br>2006-08-26 | 7.0 | CVE-2006-4368<br>FULLDISC<br>OTHER-REF<br>OTHER-REF<br>BID |

| | | | | |
|---|---|---|---|---|
| Invisionix Systems -- Invisionix Roaming System Remote | PHP remote file inclusion vulnerability in pageheaderdefault.inc.php in Invisionix Roaming System Remote (IRSR) 0.2 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the _sysSessionPath parameter. | unknown<br>2006-08-21 | 7.0 | CVE-2006-4237<br>Milw0rm<br>BID<br>XF |
| Jelsoft -- vBulletin | ** DISPUTED ** PHP remote file inclusion vulnerability in install/upgrade_301.php in Jelsoft vBulletin 3.5.4 allows remote attackers to execute arbitrary PHP code via a URL in the step parameter. NOTE: the vendor has disputed this vulnerability, saying "The default vBulletin requires authentication prior to the usage of the upgrade system." | unknown<br>2006-08-21 | 7.0 | CVE-2006-4271<br>BUGTRAQ<br>BUGTRAQ<br>BUGTRAQ<br>BUGTRAQ<br>OTHER-REF |
| Jelsoft -- vBulletin | ** DISPUTED ** Jelsoft vBulletin 3.5.4 allows remote attackers to register multiple arbitrary users and cause a denial of service (resource consumption) via a large number of requests to register.php. NOTE: the vendor has disputed this vulnerability, stating "If you have the CAPTCHA enabled then the registrations wont even go through. ... if you are talking about the flood being allowed in the first place then surely this is something that should be handled at the server level." | unknown<br>2006-08-21 | 7.0 | CVE-2006-4272<br>BUGTRAQ<br>BUGTRAQ |
| Jelsoft -- vBulletin | Cross-site scripting (XSS) vulnerability in Jelsoft vBulletin 3.5.4 and 3.6.0 allows remote attackers to inject arbitrary web script or HTML by uploading an attachment with a .pdf extension that contains JavaScript, which is processed as script by Microsoft Internet Explorer 6. | unknown<br>2006-08-21 | 7.0 | CVE-2006-4273<br>BUGTRAQ<br>BUGTRAQ<br>BUGTRAQ |
| Joomla! -- mosListMessenger component<br>Mambo -- mosListMessenger component | PHP remote file inclusion vulnerability in archive.php in the mosListMessenger Component (com_lm) before 20060719 for Mambo and Joomla! allows remote attackers to execute arbitrary PHP code via a URL in the mosConfig_absolute_path parameter. | unknown<br>2006-08-18 | 7.0 | CVE-2006-4229<br>OTHER-REF<br>OTHER-REF<br>FRSIRT<br>SECUNIA<br>BUGTRAQ |
| Joomla! -- x-shop component<br>Mambo -- x-shop component | PHP remote file inclusion vulnerability in admin.x-shop.php in the x-shop component (com_x-shop) 1.7 and earlier for Mambo and Joomla! allows remote attackers to execute arbitrary PHP code via a URL in the mosConfig_absolute_path parameter. | unknown<br>2006-08-21 | 7.0 | CVE-2006-4269<br>BUGTRAQ<br>BID<br>XF |
| Justsystem -- Ichitaro | Stack-based buffer overflow in Justsystem Ichitaro 9.x through 13.x, Ichitaro 2004, 2005, 2006, and Ichitaro for Linux allows remote attackers to execute arbitrary code via long strings in a crafted document, as being actively exploited by malware such Trojan.Tarodrop. NOTE: some details are obtained from third party information. | unknown<br>2006-08-23 | 7.0 | CVE-2006-4326<br>OTHER-REF<br>BID<br>FRSIRT<br>SECUNIA<br>XF |
| Kochsuite component -- Kochsuite component | PHP remote file inclusion vulnerability in config.kochsuite.php in the Kochsuite (com_kochsuite) 0.9.4 component for Mambo and Joomla! allows remote attackers to execute arbitrary PHP code via a URL in the mosConfig_absolute_path parameter. | unknown<br>2006-08-24 | 7.0 | CVE-2006-4348<br>BUGTRAQ<br>OTHER-REF<br>BID<br>OSVDB<br>XF |
| LBlog -- LBlog | SQL injection vulnerability in comments.asp in LBlog 1.05 and earlier allows remote attackers to execute arbitrary SQL commands via the id parameter. | unknown<br>2006-08-22 | 7.0 | CVE-2006-4284<br>OTHER-REF<br>BID<br>SECUNIA<br>BUGTRAQ<br>SECTRACK<br>XF |
| Linux -- Linux kernel | Unspecified vulnerability in the SCTP implementation in Linux 2.6.9, and probably other 2.6.x versions, allows local users to cause a denial of service (panic) and possibly gain root privileges. via attack vectors. | unknown<br>2006-08-23 | 7.0 | CVE-2006-3745<br>REDHAT<br>SECUNIA |
| Lizge -- Lizge Web Portal | Multiple PHP remote file inclusion vulnerabilities in index.php in Lizge V.20 Web Portal allow remote attackers to execute arbitrary PHP code via a URL in the (1) lizge or (2) bade parameters. | unknown<br>2006-08-18 | 7.0 | CVE-2006-4230<br>BUGTRAQ<br>BID<br>XF |
| Mambo -- mtg_myhomepage Component | Multiple PHP remote file inclusion vulnerabilities in the mtg_myhomepage Component (com_lmtg_myhomepage) for Mambo allow remote attackers to execute arbitrary PHP code via a URL in the mosConfig_absolute_path parameter in (1) install.lmtg_homepage.php and (2) mtg_homepage.php. | unknown<br>2006-08-21 | 7.0 | CVE-2006-4264<br>BUGTRAQ |
| Mambo -- mambelfish component | PHP remote file inclusion vulnerability in mambelfish.class.php in the mambelfish component (com_mambelfish) 1.1 and earlier for Mambo allows remote attackers to execute arbitrary PHP code via a URL in the mosConfig_absolute_path parameter. | unknown<br>2006-08-21 | 7.0 | CVE-2006-4270<br>BUGTRAQ<br>OTHER-REF<br>FRSIRT<br>SECUNIA<br>XF |

| | | | | |
|---|---|---|---|---|
| Mambo -- CatalogShop component | PHP remote file inclusion vulnerability in catalogshop.php in the CatalogShop component for Mambo (com_catalogshop) allows remote attackers to execute arbitrary PHP code via a URL in the mosConfig_absolute_path parameter. | unknown<br>2006-08-21 | 7.0 | CVE-2006-4275<br>BUGTRAQ<br>BID |
| Mambo -- ANJEL Component | PHP remote file inclusion vulnerability in anjel.index.php in ANJEL (formerly MaMML) Component (com_anjel) for Mambo allows remote attackers to execute arbitrary PHP code via a URL in the mosConfig_absolute_path parameter. | unknown<br>2006-08-21 | 7.0 | CVE-2006-4280<br>BUGTRAQ<br>XF |
| Mambo -- Mambo | PHP remote file inclusion vulnerability in contentpublisher.php in the contentpublisher component (com_contentpublisher) for Mambo allows remote attackers to execute arbitrary PHP code via a URL in the mosConfig_absolute_path parameter. | unknown<br>2006-08-22 | 7.0 | CVE-2006-4286<br>BUGTRAQ |
| Mambo -- a6mambocredits component | PHP remote file inclusion vulnerability in admin.a6mambocredits.php in the a6mambocredits component (com_a6mambocredits) 2.0.0 and earlier for Mambo allows remote attackers to execute arbitrary PHP code via a URL in the mosConfig_live_site parameter. NOTE: some of these details are obtained from third party information. | unknown<br>2006-08-22 | 7.0 | CVE-2006-4288<br>OTHER-REF<br>BID<br>FRSIRT<br>SECTRACK<br>SECUNIA<br>XF |
| Mambo -- bigAPE-Backup component | PHP remote file inclusion vulnerability in classes/Tar.php in bigAPE-Backup component (com_babackup) for Mambo 1.1 allows remote attackers to include arbitrary files via the mosConfig_absolute_path parameter. | unknown<br>2006-08-22 | 7.0 | CVE-2006-4296<br>OTHER-REF<br>BID<br>FRSIRT<br>SECUNIA<br>XF |
| MamboXChange -- Reporter | PHP remote file inclusion vulnerability in processor/reporter.sql.php in the Reporter Mambo component (com_reporter) allows remote attackers to execute arbitrary PHP code via a URL in the mosConfig_absolute_path parameter. | unknown<br>2006-08-21 | 7.0 | CVE-2006-4241<br>BUGTRAQ<br>BID<br>XF |
| MamboXChange -- MamboWiki | PHP remote file inclusion vulnerability in MamboLogin.php in the MamboWiki component (com_mambowiki) 0.9.6 and earlier for Mambo and Joomla! allows remote attackers to execute arbitrary PHP code via a URL in the IP parameter. | unknown<br>2006-08-22 | 7.0 | CVE-2006-4282<br>BUGTRAQ<br>OTHER-REF<br>OTHER-REF<br>BID |
| Microsoft -- Internet Explorer | Buffer overflow in Microsoft Internet Explorer 6 SP1 on Windows 2000 and XP SP1 with MS06-042 allows remote attackers to cause a denial of service (crash) or execute arbitrary code via a long URL on a website that uses HTTP 1.1 compression. | unknown<br>2006-08-22 | 7.0 | CVE-2006-3869<br>BUGTRAQ<br>OTHER-REF<br>OTHER-REF<br>CERT-VN<br>SECTRACK |
| Mozilla -- Firefox | Mozilla Firefox 1.5.0.6 and earlier allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a series of Javascript timed events that load an XML file containing a large number of closing tags, which triggers a memory fault, aka ffoxdie3. NOTE: this is very similar to CVE-2006-4253, but possibly a different issue. | unknown<br>2006-08-21 | 7.0 | CVE-2006-4261<br>BUGTRAQ<br>OTHER-REF |
| NES Game -- NES Game<br>NES System -- NES System | Multiple PHP remote file inclusion vulnerabilities in NES Game and NES System c108122 and earlier allow remote attackers to execute arbitrary PHP code via a URL in the (1) phphtmllib parameter to (a) phphtmllib/includes.php; tag_utils/ scripts including (b) divtag_utils.php, (c) form_utils.php, (d) html_utils.php, and (e) localinc.php; and widgets/ scripts including (f) FooterNav.php, (g) HTMLPageClass.php, (h) InfoTable.php, (i) localinc.php, (j) NavTable.php, and (k) TextNav.php. | unknown<br>2006-08-22 | 7.0 | CVE-2006-4287<br>OTHER-REF<br>OTHER-REF<br>BID<br>SECUNIA<br>FRSIRT<br>OSVDB<br>OSVDB<br>OSVDB<br>OSVDB<br>OSVDB<br>OSVDB<br>OSVDB<br>OSVDB<br>OSVDB<br>OSVDB<br>OSVDB |
| OneOrZero -- OneOrZero | SQL injection vulnerability in index.php in OneOrZero 1.6.4.1 allows remote attackers to execute arbitrary SQL commands via the id parameter. | unknown<br>2006-08-24 | 7.0 | CVE-2006-4350<br>BUGTRAQ |
| OneOrZero -- OneOrZero | Cross-site scripting (XSS) vulnerability in index.php in OneOrZero 1.6.4.1 allows remote attackers to inject arbitrary web script or HTML via the id parameter. | unknown<br>2006-08-24 | 7.0 | CVE-2006-4351<br>BUGTRAQ |

| | | | | |
|---|---|---|---|---|
| OpenSEF Project -- OpenSEF | PHP remote file inclusion vulnerability in sef.php in the OpenSEF 2.0.0 component for Joomla! allows remote attackers to execute arbitrary PHP code via a URL in the mosConfig_absolute_path parameter. | unknown<br>2006-08-23 | 7.0 | CVE-2006-4320<br>BUGTRAQ<br>BID<br>SECTRACK<br>XF |
| osCommerce -- osCommerce | SQL injection vulnerability in shopping_cart.php in osCommerce 2.2 Milestone 2 060817 allows remote attackers to execute arbitrary SQL commands via id array parameters. | unknown<br>2006-08-22 | 7.0 | CVE-2006-4297<br>OTHER-REF<br>BID<br>SECTRACK<br>XF |
| Outreach Project Tool -- OPT Max | PHP remote file inclusion vulnerability in include/urights.php in Outreach Project Tool (OPT) Max 1.2.6 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the CRM_inc parameter. | unknown<br>2006-08-21 | 7.0 | CVE-2006-4239<br>Milw0rm<br>BID<br>FRSIRT<br>SECUNIA<br>XF |
| Phome Empire -- Phome Empire CMS | PHP remote file inclusion vulnerability in e/class/CheckLevel.php in Phome Empire CMS 3.7 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the check_path parameter. | unknown<br>2006-08-26 | 7.0 | CVE-2006-4354<br>OTHER-REF<br>BID<br>SECUNIA<br>XF |
| Powergap -- Powergap Lite<br>Powergap -- Powergap Business | Multiple PHP remote file inclusion vulnerabilities in POWERGAP allow remote attackers to execute arbitrary PHP code via a URL in the (1) shopid parameter to (a) s01.php, (b) s02.php, (c) s03.php, or (d) s04.php; or (2) sid parameter to (e) index.php. | unknown<br>2006-08-21 | 7.0 | CVE-2006-4236<br>BUGTRAQ<br>Milw0rm<br>BID<br>XF<br>SECTRACK |
| Product Scroller Module -- Product Scroller Module | Multiple PHP remote file inclusion vulnerabilities in the Product Scroller Module and other modules in mambo-phpshop (com_phpshop) for Mambo and Joomla! allow remote attackers to execute arbitrary PHP code via a URL in the mosConfig_absolute_path parameter in (1) mod_phpshop.php, (2) mod_phpshop_allinone.php, (3) mod_phpshop_cart.php, (4) mod_phpshop_featureprod.php, (5) mod_phpshop_latestprod.php, (6) mod_product_categories.php, (7) mod_productscroller.php, and (8) mosproductsnap.php. | unknown<br>2006-08-21 | 7.0 | CVE-2006-4263<br>BUGTRAQ<br>BID |
| RedBLoG -- RedBLoG | PHP remote file inclusion vulnerability in index.php in RedBLoG 0.5 allows remote attackers to execute arbitrary PHP code via a URL in the root_path parameter. NOTE: the provenance of this information is unknown; the details are obtained from third party information. | unknown<br>2006-08-26 | 7.0 | CVE-2006-4366<br>OTHER-REF<br>BID |
| Rssxt component -- Rssxt component | ** DISPUTED ** Multiple PHP remote file inclusion vulnerabilities in the Rssxt component for Joomla! (com_rssxt), possibly 2.0 Beta 1 or 1.0 and earlier, allow remote attackers to execute arbitrary PHP code via a URL in the mosConfig_absolute_path parameter in (1) pinger.php, (2) RPC.php, or (3) rssxt.php. NOTE: another researcher has disputed this issue, saying that the attacker can not control this parameter. In addition, as of 20060825, the original researcher has appeared to be unreliable with some other past reports. CVE has not performed any followup analysis with respect to this issue. | unknown<br>2006-08-26 | 7.0 | CVE-2006-4378<br>BUGTRAQ<br>BUGTRAQ |
| Shadows Rising RPG -- Shadows Rising RPG | Multiple PHP remote file inclusion vulnerabilities in Shadows Rising RPG (Pre-Alpha) 0.0.5b and earlier allow remote attackers to execute arbitrary PHP code via a URL in the CONFIG[gameroot] parameter to (1) core/includes/security.inc.php, (2) core/includes/smarty.inc.php, (3) qcms/includes/smarty.inc.php or (4) qlib/smarty.inc.php. | unknown<br>2006-08-23 | 7.0 | CVE-2006-4329<br>MLIST<br>OTHER-REF<br>BID<br>XF |
| SOLMETRA -- SPAW Editor | Multiple PHP remote file inclusion vulnerabilities in SOLMETRA SPAW Editor 1.0.6 and 1.0.7 allow remote attackers to execute arbitrary PHP code via a URL in the spaw_dir parameter in dialogs/ scripts including (1) a.php, (2) collorpicker.php, (3) img.php, (4) img_library.php, (5) table.php, or (6) td.php. | unknown<br>2006-08-22 | 7.0 | CVE-2006-4283<br>BUGTRAQ<br>BID |
| Sonium -- Enterprise Adressbook | PHP remote file inclusion vulnerability in Sonium Enterprise Adressbook 0.2 allows remote attackers to execute arbitrary PHP code via the folder parameter in multiple files in the plugins directory, as demonstrated by plugins/1_Adressbuch/delete.php. | unknown<br>2006-08-23 | 7.0 | CVE-2006-4311<br>OTHER-REF<br>FRSIRT<br>SECUNIA<br>XF |
| Sony -- SonicStage Mastering Studio | Buffer overflow in the import project functionality in Sony SonicStage Mastering Studio 1.1.00 through 2.2.01 allows remote attackers to execute arbitrary code via a crafted SMP file. | unknown<br>2006-08-21 | 7.0 | CVE-2006-4235<br>PENTEST<br>OTHER-REF<br>CERT-VN<br>BID<br>FRSIRT<br>OSVDB<br>SECUNIA |

|  |  |  |  |  |
|---|---|---|---|---|
|  |  |  |  | XF |
| Sony -- VAIO Media Server | Buffer overflow in Sony VAIO Media Server 2.x, 3.x, 4.x, and 5.x before 20060626 allows remote attackers to execute arbitrary code via unspecified vectors. | unknown<br>2006-08-22 | 10.0 | CVE-2006-4289<br>OTHER-REF<br>OTHER-REF<br>OTHER-REF<br>BID<br>FRSIRT<br>SECUNIA<br>XF |
| SportsPHool -- SportsPHool | PHP remote file inclusion vulnerability in includes/layout/plain.footer.php in SportsPHool 1.0 allows remote attackers to execute arbitrary PHP code via a URL in the mainnav parameter. | unknown<br>2006-08-21 | 7.0 | CVE-2006-4278<br>OTHER-REF<br>BID<br>SECUNIA<br>FRSIRT<br>XF |
| SSH Communications Security -- Tectia Client<br>SSH Communications Security -- SSH Tectia Manager<br>SSH Communications Security -- Tectia Server<br>SSH Communications Security -- Tectia Manager<br>SSH Communications Security -- Tectia Connector | Unquoted Windows search path vulnerability in multiple SSH Tectia products, including Client/Server/Connector 5.0.0 and 5.0.1 and Client/Server before 4.4.5, and Manager 2.12 and earlier, when running on Windows, might allow local users to gain privileges via a malicious program file under "Program Files" or its subdirectories. | unknown<br>2006-08-23 | 7.0 | CVE-2006-4315<br>OTHER-REF<br>BID |
| SSH Communications Security -- SSH Tectia Manager | SSH Tectia Management Agent 2.1.2 allows local users to gain root privileges by running a program called sshd, which is obtained from a process listing when the "Restart" action is selected from the Management server GUI, which causes the agent to locate the pathname of the user's program and restart it with root privileges. | unknown<br>2006-08-23 | 7.0 | CVE-2006-4316<br>OTHER-REF<br>BID |
| Streamripper -- Streamripper | Buffer overflow in the HTTP header parsing in Streamripper before 1.61.26 allows remote attackers to cause a denial of service and possibly execute arbitrary code via crafted HTTP headers. | unknown<br>2006-08-26 | 7.0 | CVE-2006-3124<br>OTHER-REF<br>BID<br>FRSIRT<br>SECUNIA<br>XF |
| Sun -- Solaris | Unspecified vulnerability in Sun Solaris 8 and 9 before 20060821 allows local users to execute arbitrary commands via unspecified vectors, involving the default Role-Based Access Control (RBAC) settings in the "File System Management" profile. | unknown<br>2006-08-23 | 7.0 | CVE-2006-4306<br>SUNALERT<br>BID<br>SECTRACK |
| Sun -- Solaris | Unspecified vulnerability in the format command in Sun Solaris 8 and 9 before 20060821 allows local users to modify arbitrary files via unspecified vectors involving profiles that permit running format with elevated privileges, a different issue than CVE-2006-4306. | unknown<br>2006-08-23 | 7.0 | CVE-2006-4307<br>SUNALERT<br>BID<br>SECTRACK |
| Texas Imperial Software -- WFTPD | Buffer overflow in WFTPD Server 3.23 allows remote attackers to execute arbitrary code via long SIZE commands. | unknown<br>2006-08-23 | 7.0 | CVE-2006-4318<br>OTHER-REF<br>BID<br>SECTRACK |
| Toenda Software Development -- toendaCMS | ** DISPUTED ** PHP remote file inclusion vulnerability in ToendaCMS 1.0.3 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the tcms_administer_site parameter to an unspecified script, probably index.php. NOTE: this issue has been disputed by a third party, who states that $tcms_administer_site is initialized to a constant value within index.php. | unknown<br>2006-08-24 | 7.0 | CVE-2006-4349<br>BUGTRAQ<br>BUGTRAQ<br>BID<br>XF |
| Tutti Nova -- Tutti Nova | PHP remote file inclusion vulnerability in Tutti Nova 1.6 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the TNLIB_DIR parameter to novalib/class.novaEdit.mysql.php. | unknown<br>2006-08-21 | 7.0 | CVE-2006-4276<br>OTHER-REF<br>BID<br>SECUNIA<br>FRSIRT<br>XF |
| Tutti Nova -- Tutti Nova | Multiple PHP remote file inclusion vulnerabilities in Tutti Nova 1.6 and earlier allow remote attackers to execute arbitrary PHP code via a URL in the TNLIB_DIR parameter to (1) include/novalib/class.novaAdmin.mysql.php and (2) novalib/class.novaRead.mysql.php. NOTE: the provenance of this information is unknown; the details are obtained from third party information. | unknown<br>2006-08-21 | 7.0 | CVE-2006-4277<br>BID<br>SECUNIA |
| VistaBB -- VistaBB | Multiple PHP remote file inclusion vulnerabilities in VistaBB 2.0.33 and earlier allow remote attackers to execute arbitrary PHP code via a URL in the phpbb_root_path parameter in (1) includes/functions_mod_user.php or (2) includes/functions_portal.php. | unknown<br>2006-08-26 | 7.0 | CVE-2006-4365<br>FULLDISC<br>OTHER-REF<br>OTHER-REF<br>BID |

| | | | | |
|---|---|---|---|---|
| | | | | FRSIRT<br>SECUNIA |
| VWar -- Virtual War | Multiple SQL injection vulnerabilities in war.php in Virtual War (VWar) 1.5.0 and earlier allow remote attackers to execute arbitrary SQL commands via the (1) s, (2) showgame, (3) sortby, and (4) sortorder parameters. NOTE: The page parameter vector is covered by CVE-2006-4010. | unknown<br>2006-08-18 | 7.0 | CVE-2006-4225<br>BUGTRAQ |
| Woltlab -- Burning Board | Cross-site scripting (XSS) vulnerability in attachment.php in WoltLab Burning Board (WBB) 2.3.5 allows remote attackers to inject arbitrary web script or HTML via a GIF image that contains URL-encoded Javascript. | unknown<br>2006-08-23 | 7.0 | CVE-2006-4317<br>BUGTRAQ<br>BID<br>XF |
| WTCom -- Web Torrent | SQL injection vulnerability in torrents.php in WebTorrent (WTcom) 0.2.4 and earlier allows remote attackers to execute arbitrary SQL commands via the cat parameter in category mode. | unknown<br>2006-08-21 | 7.0 | CVE-2006-4238<br>Milw0rm<br>BID<br>XF |
| XennoBB -- XennoBB | SQL injection vulnerability in topic_post.php in XennoBB 2.2.1 and earlier allows remote attackers to execute arbitrary SQL commands via the icon_topic parameter. | unknown<br>2006-08-21 | 7.0 | CVE-2006-4279<br>BUGTRAQ<br>OTHER-REF<br>BID<br>FRSIRT<br>SECUNIA<br>XF |

Back to top

## Medium Vulnerabilities

| Primary<br>Vendor -- Product | Description | Discovered<br>Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| Apple -- Mac OS X Server<br>Apple -- Mac OS X<br>Apple -- Xsan | Buffer overflow in the Xsan Filesystem driver on Mac OS X 10.4.7 and OS X Server 10.4.7 allows local users with Xsan write access, to execute arbitrary code via unspecified vectors related to "processing a path name." | unknown<br>2006-08-21 | 4.9 | CVE-2006-3506<br>APPLE<br>BID<br>FRSIRT<br>SECTRACK<br>SECUNIA<br>CERT-VN |
| Cisco -- PIX Firewall<br>Cisco -- Adaptive Security Appliance | Cisco PIX 500 Series Security Appliances and ASA 5500 Series Adaptive Security Appliances, when running 7.0(x) up to 7.0(5) and 7.1(x) up to 7.1(2.4), and Firewall Services Module (FWSM) 3.1(x) up to 3.1(1.6), causes the EXEC password, local user passwords, and the enable password to be changed to a "non-random value" under certain circumstances, which causes administrators to be locked out and might allow attackers to gain access. | unknown<br>2006-08-23 | 4.2 | CVE-2006-4312<br>CISCO |
| Cscope -- Cscope | Multiple buffer overflows in cscope 15.5 and earlier allow user-assisted attackers to cause a denial of service (crash) and possibly execute arbitrary code via multiple vectors including (1) a long pathname that is not properly handled during file list parsing, (2) long pathnames that result from path variable expansion such as tilde expansion for the HOME environment variable, and (3) command line argument. | unknown<br>2006-08-23 | 5.6 | CVE-2006-4262<br>OTHER-REF<br>OTHER-REF |
| Drupal -- Drupal Easylinks Module | Cross-site scripting (XSS) vulnerability in Drupal Easylinks Module (easylinks.module) 4.7 before 1.5.2.1 2006/08/19 12:02:27 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. | unknown<br>2006-08-26 | 5.6 | CVE-2006-4355<br>OTHER-REF<br>BID<br>SECUNIA |
| Drupal -- Drupal Easylinks Module | SQL injection vulnerability in Drupal Easylinks Module (easylinks.module) 4.7 before 1.5.2.1 2006/08/19 12:02:27 allows remote attackers to execute arbitrary SQL commands via unspecified vectors. | unknown<br>2006-08-26 | 5.6 | CVE-2006-4356<br>OTHER-REF<br>BID<br>SECUNIA |
| Drupal -- Drupal E-commerce Module | Cross-site scripting (XSS) vulnerability in E-commerce 4.7 for Drupal before file.module 1.37.2.4 (20060812) allows remote authenticated users with the "create products" permission to inject arbitrary web script or HTML via unspecified vectors. | unknown<br>2006-08-26 | 4.2 | CVE-2006-4360<br>OTHER-REF<br>BID<br>SECUNIA |
| Fuji Xerox -- Fuji Xerox Printing Systems (FXPS) print engine | The embedded HTTP server in Fuji Xerox Printing Systems (FXPS) print engine, as used in products including Dell 3000cn through 5110cn, does not properly perform authentication for HTTP requests, which allows remote attackers to modify system configuration via crafted requests, including changing the administrator password or causing a denial of service to the print server. | unknown<br>2006-08-24 | 4.7 | CVE-2006-2113<br>OTHER-REF |
| ImageMagick -- ImageMagick | Multiple buffer overflows in ImageMagick before 6.2.9 allow user-assisted attackers to execute arbitrary code via crafted XCF images. | unknown<br>2006-08-24 | 5.6 | CVE-2006-3743<br>OTHER-REF<br>REDHAT<br>SECUNIA |

| | | | | |
|---|---|---|---|---|
| ImageMagick -- ImageMagick | Multiple integer overflows in ImageMagick before 6.2.9 allows user-assisted attackers to execute arbitrary code via crafted Sun bitmap images that trigger heap-based buffer overflows. | unknown<br>2006-08-24 | 5.6 | CVE-2006-3744<br>OTHER-REF<br>REDHAT<br>SECUNIA |
| Joomla! -- JIM Instant Messaging Component | PHP remote file inclusion vulnerability in install.jim.php in the JIM 1.0.1 component for Joomla or Mambo allows remote attackers to execute arbitrary PHP code via a URL in the mosConfig_absolute_path parameter. | unknown<br>2006-08-21 | 5.6 | CVE-2006-4242<br>BUGTRAQ<br>Milw0rm<br>BID<br>FRSIRT<br>OSVDB<br>SECUNIA<br>XF |
| Microsoft -- PowerPoint | Unknown vulnerability in Microsoft PowerPoint allows user-assisted attackers to execute arbitrary code via a crafted PPT document, as being actively exploited by malware such as TROJ_MDROPPER.BH. NOTE: as of 20060821, it has been reported that this is a different issue than CVE-2006-3660, CVE-2006-3656, and CVE-2006-3655. | unknown<br>2006-08-21 | 5.6 | CVE-2006-4274<br>BUGTRAQ<br>OTHER-REF<br>OTHER-REF<br>OTHER-REF<br>SECTRACK |
| Mozilla -- Firefox | Mozilla Firefox 1.5.0.6 and earlier allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via multiple Javascript timed events that load a deeply nested XML file, followed by redirecting the browser to another page, which leads to a concurrency failure that causes structures to be freed incorrectly, as demonstrated by ffoxdie. NOTE: it has been reported that Netscape 8.1 and K-Meleon 1.0.1 are also affected. | unknown<br>2006-08-21 | 5.6 | CVE-2006-4253<br>BUGTRAQ<br>BUGTRAQ<br>BUGTRAQ<br>BUGTRAQ<br>OTHER-REF<br>BID<br>SECUNIA<br>OTHER-REF<br>BID |
| MySQL -- MySQL | MySQL before 5.0.25 and 5.1 before 5.1.12 evaluates arguments of suid routines in the security context of the routine's definer instead of the routine's caller, which allows remote authenticated users to gain privileges through a routine that has been made available using GRANT EXECUTE. | unknown<br>2006-08-18 | 4.2 | CVE-2006-4227<br>MLIST<br>OTHER-REF<br>BID<br>FRSIRT<br>SECUNIA<br>OTHER-REF<br>SECTRACK<br>XF |
| PHlyMail -- PHlyMail Lite | PHP remote file inclusion vulnerability in handlers/email/mod.listmail.php in PHlyMail Lite 3.4.4 and earlier (Build 3.04.04) allows remote attackers to execute arbitrary PHP code via a URL in the _PM_[path][handler] parameter. | unknown<br>2006-08-22 | 5.6 | CVE-2006-4291<br>OTHER-REF<br>BID<br>SECTRACK<br>SECUNIA<br>XF |
| Sun -- Solaris | Buffer overflow in the format command in Solaris 8, 9, and 10 allows local users with access to format (such as the "File System Management" RBAC profile) to execute arbitrary code via unknown vectors, a different vulnerability than CVE-2006-4307. | unknown<br>2006-08-23 | 4.9 | CVE-2006-4319<br>SUNALERT |
| Trident Software -- PowerZip | Stack-based buffer overflow in Trident Software PowerZip 7.06 Build 3895 on Windows 2000 allows remote attackers to execute arbitrary code via a ZIP archive containing a long filename. | unknown<br>2006-08-26 | 5.6 | CVE-2006-4359<br>BID<br>SECUNIA |

Back to top

## Low Vulnerabilities

| Primary<br>Vendor -- Product | Description | Discovered<br>Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| Alt-N -- MDaemon | Multiple heap-based buffer overflows in the POP3 server in Alt-N Technologies MDaemon before 9.0.6 allow remote attackers to cause a denial of service (daemon crash) and possibly execute arbitrary code via long strings that contain '@' characters in the (1) USER and (2) APOP commands. | unknown<br>2006-08-26 | 2.3 | CVE-2006-4364<br>BUGTRAQ<br>OTHER-REF<br>OTHER-REF<br>OTHER-REF<br>BID<br>SECTRACK<br>SECUNIA<br>XF |
| Alt-N -- WebAdmin | Multiple directory traversal vulnerabilities in Alt-N WebAdmin 3.2.3 and 3.2.4 running with MDaemon 9.0.5, and possibly earlier, allow remote authenticated global administrators to read arbitrary files via a .. (dot dot) in the file parameter to (1) logfile_view.wdm and (2) configfile_view.wdm. | unknown<br>2006-08-26 | 2.3 | CVE-2006-4371<br>BUGTRAQ<br>FULLDISC<br>OTHER-REF |

| | | | | |
|---|---|---|---|---|
| | | | | BID<br>FRSIRT<br>SECUNIA<br>XF |
| Blackboard -- Blackboard<br>Blackboard -- Blackboard Learning and Community Portal Suite | Multiple cross-site scripting (XSS) vulnerabilities in Blackboard Learning System 6 and Blackboard Learning and Community Portal Suite 6.2.3.23 allow remote attackers to inject arbitrary Javascript, VBScript, or HTML via (1) data, (2) vbscript, and (3) malformed javascript URIs in various HTML tags when posting to the Discussion Board. | unknown<br>2006-08-23 | 2.3 | CVE-2006-4308<br>BUGTRAQ<br>BID<br>SECUNIA |
| CGI-RESCUE -- Mail F/W System | CRLF injection vulnerability in CGI-Rescue Mail F/W System (formd) before 8.3 allows remote attackers to spoof e-mails and inject e-mail headers via unspecified vectors in (1) mail.cgi and (2) query.cgi. | unknown<br>2006-08-24 | 2.3 | CVE-2006-4344<br>OTHER-REF<br>OTHER-REF<br>BID<br>FRSIRT<br>OSVDB |
| Cisco -- VPN 3000 Concentrator | Multiple unspecified vulnerabilities in Cisco VPN 3000 series concentrators before 4.1, 4.1.x up to 4.1(7)L, and 4.7.x up to 4.7(2)F allow attackers to execute the (1) CWD, (2) MKD, (3) CDUP, (4) RNFR, (5) SIZE, and (6) RMD FTP commands to modify files or create and delete directories via unknown vectors. | unknown<br>2006-08-23 | 2.3 | CVE-2006-4313<br>CISCO |
| Cisco -- Content Service Switch | The ArrowPoint cookie functionality for Cisco 11000 series Content Service Switches specifies an internal IP address if the administrator does not specify a string option, which allows remote attackers to obtain sensitive information. | unknown<br>2006-08-25 | 2.3 | CVE-2006-4352<br>OSVDB<br>OTHER-REF |
| cPanel -- cPanel | Multiple cross-site scripting (XSS) vulnerabilities in cPanel 10 allow remote attackers to inject arbitrary web script or HTML via the (1) dir parameter in dohtaccess.html, or the (2) file parameter in (a) editit.html or (b) showfile.html. | unknown<br>2006-08-22 | 2.3 | CVE-2006-4293<br>BUGTRAQ<br>SECUNIA<br>XF |
| Fuji Xerox -- Fuji Xerox Printing Systems (FXPS) print engine | Fuji Xerox Printing Systems (FXPS) print engine, as used in products including Dell 3000cn through 5110cn, allows remote attackers to use the FTP printing interface as a proxy ("FTP bounce") by using arbitrary PORT arguments to connect to systems for which access would be otherwise restricted. | unknown<br>2006-08-24 | 2.3 | CVE-2006-2112<br>OTHER-REF |
| Globus -- Globus Toolkit | Race condition in the grid-proxy-init tool in Globus Toolkit 3.2.x, 4.0.x, and 4.1.0 before 20060815 allows local users to steal credential data by replacing the proxy credentials file in between file creation and the check for exclusive file access. | unknown<br>2006-08-18 | 1.3 | CVE-2006-4232<br>MLIST<br>BID<br>FRSIRT<br>SECUNIA<br>XF |
| Globus -- Globus Toolkit | Globus Toolkit 3.2.x, 4.0.x, and 4.1.0 before 20060815 allow local users to obtain sensitive information (proxy certificates) and overwrite arbitrary files via a symlink attack on temporary files in the /tmp directory, as demonstrated by files created by (1) myproxy-admin-adduser, (2) grid-ca-sign, and (3) grid-security-config. | unknown<br>2006-08-18 | 3.3 | CVE-2006-4233<br>MLIST<br>BID<br>FRSIRT<br>SECUNIA<br>XF |
| Horde -- IMP<br>Horde -- Horde | Cross-site scripting (XSS) vulnerability in horde/imp/search.php in Horde IMP H3 before 4.1.3 allows remote attackers to include arbitrary web script or HTML via multiple unspecified vectors related to folder names, as injected into the vfolder_label form field in the IMP search screen. | unknown<br>2006-08-21 | 2.3 | CVE-2006-4255<br>BUGTRAQ<br>MLIST<br>OTHER-REF<br>BID<br>FRSIRT<br>SECUNIA<br>XF |
| Horde -- Application Framework | index.php in Horde Application Framework before 3.1.2 allows remote attackers to include web pages from other sites, which could be useful for phishing attacks, via a URL in the url parameter, aka "cross-site referencing." NOTE: some sources have referred to this issue as XSS, but it is different than classic XSS. | unknown<br>2006-08-21 | 2.3 | CVE-2006-4256<br>BUGTRAQ<br>MLIST<br>OTHER-REF<br>FRSIRT<br>SECUNIA<br>XF |
| IBM -- WebSphere Application Server | IBM WebSphere Application Server before 6.0.2.13 allows context-dependent attackers to obtain sensitive information via unspecified vectors related to (1) "JSP source code exposure" (PK23475), (2) the First Failure Data Capture (ffdc) log file (PK24834), and (3) traces (PK25568), a different issue than CVE-2006-4137. | unknown<br>2006-08-18 | 2.3 | CVE-2006-4223<br>OTHER-REF<br>FRSIRT<br>SECUNIA |
| IBM -- DB2 Universal Database | Unspecified vulnerability in IBM DB2 Universal Database (UDB) before 8.1 FixPak 13 allows remote authenticated users to cause a denial of service via unspecified vectors (1) during the "CONNECT / ATTACH" or (2) after the CONNECT processing. NOTE: some details have been obtained from third parties. | unknown<br>2006-08-21 | 1.4 | CVE-2006-4257<br>OTHER-REF<br>SECUNIA<br>AIXAPAR<br>FRSIRT<br>OSVDB |

| | | | | |
|---|---|---|---|---|
| | | | | OSVDB |
| IntegraMOD -- IntegraMOD Portal | Absolute path traversal vulnerability in includes/functions_portal.php in IntegraMOD Portal 2.x and earlier, when magic_quotes_gpc is disabled, allows remote attackers to read arbitrary files via an absolute pathname in the phpbb_root_path parameter. | unknown<br>2006-08-26 | 2.3 | CVE-2006-4369<br>FULLDISC<br>OTHER-REF<br>OTHER-REF<br>BID |
| Irfan Skiljan -- IrfanView32 | IrfanView 3.98 (with plugins) allows remote attackers to cause a denial of service (application crash) via a crafted CUR image file. | unknown<br>2006-08-18 | 1.9 | CVE-2006-4231<br>BUGTRAQ<br>XF |
| Irfan Skiljan -- IrfanView32 | IrfanView 3.98 (with plugins) allows user-assisted attackers to cause a denial of service (application crash) via a crafted ANI image file, possibly due to a buffer overflow. | unknown<br>2006-08-26 | 1.9 | CVE-2006-4374<br>BUGTRAQ<br>BID<br>XF |
| Jake Olefsky -- Fotopholder | Cross-site scripting (XSS) vulnerability in index.php in Fotopholder 1.8 allows remote attackers to inject arbitrary web script or HTML via the path parameter. NOTE: this might be resultant from a directory traversal vulnerability. | unknown<br>2006-08-21 | 1.9 | CVE-2006-4259<br>BUGTRAQ<br>SECTRACK<br>XF |
| Jake Olefsky -- Fotopholder | Directory traversal vulnerability in index.php in Fotopholder 1.8 allows remote attackers to read arbitrary directories or files via a .. (dot dot) in the path parameter. | unknown<br>2006-08-21 | 2.3 | CVE-2006-4260<br>BUGTRAQ<br>SECTRACK<br>XF |
| Jiran -- Cool Messenger Office/School Server<br>Jiran -- Cool Manager | SQL injection vulnerability in user logon authentication request handling in Cool_CoolD.exe in Cool Manager 5.0 (5,60,90,28) and Cool Messenger Office/School Server 5.5 (5,65,12,13) allows remote attackers to execute arbitrary SQL commands via the username field. | 2006-07-15<br>2006-08-24 | 2.3 | CVE-2006-4347<br>OTHER-REF<br>BID<br>SECUNIA |
| John Hanna -- Anti-Spam SMTP Proxy Server | Absolute path traversal vulnerability in the get functionality in Anti-Spam SMTP Proxy (ASSP) allows remote authenticated users to read arbitrary files via (1) C:\ (Windows drive letter), (2) UNC, and possibly other types of paths in the file parameter. | unknown<br>2006-08-21 | 1.4 | CVE-2006-4258<br>FULLDISC<br>BID<br>FRSIRT<br>SECUNIA<br>XF |
| Kaspersky Lab -- Kaspersky Anti-Hacker | Kaspersky Anti-Hacker 1.8.180, when Stealth Mode is enabled, allows remote attackers to obtain responses to ICMP (1) timestamp and (2) netmask requests, which is inconsistent with the documented behavior of Stealth Mode. | unknown<br>2006-08-21 | 2.3 | CVE-2006-4265<br>BUGTRAQ |
| Linux -- Linux kernel | Unspecified vulnerability in the restore_all code path of the 4/4GB split support for non-hugemem Linux kernels 2.6.9, and probably other 2.6.x versions, allows local users to cause a denial of service (panic) via unspecified vectors. | unknown<br>2006-08-23 | 2.3 | CVE-2006-2932<br>REDHAT<br>SECUNIA |
| Linux -- Linux kernel | Linux kernel 2.x.6 before 2.6.17.9 and 2.4.x before 2.4.33.1 on PowerPC PPC970 systems allows local users to cause a denial of service (crash) related to the "HID0 attention enable on PPC970 at boot time." | unknown<br>2006-08-21 | 2.3 | CVE-2006-4093<br>OTHER-REF<br>OTHER-REF<br>FRSIRT<br>BID<br>FRSIRT<br>SECUNIA |
| Microsoft -- Internet Explorer | Microsoft Internet Explorer 6.0 SP1 allows remote attackers to cause a denial of service (crash) via a long Color attribute in multiple ActiveX COM Objects from (a) dxtmsft.dll and (b)dxtmsft3.dll, including (1) DXImageTransform.Microsoft.MaskFilter.1, (2) DXImageTransform.Microsoft.Chroma.1, and (3) DX3DTransform.Microsoft.Shapes.1. | unknown<br>2006-08-22 | 2.3 | CVE-2006-4301<br>BUGTRAQ<br>OTHER-REF<br>BID |
| Mozilla -- Firefox | Mozilla Firefox 1.5.0.6 allows remote attackers to cause a denial of service (crash) via a crafted FTP response, when attempting to connect with a username and password via the FTP URI. | unknown<br>2006-08-23 | 2.3 | CVE-2006-4310<br>BUGTRAQ<br>BID |
| MySQL -- MySQL | MySQL before 4.1.21, 5.0 before 5.0.25, and 5.1 before 5.1.12, when run on case-sensitive filesystems, allows remote authenticated users to create or access a database when the database name differs only in case from a database for which they have permissions. | unknown<br>2006-08-18 | 2.2 | CVE-2006-4226<br>MLIST<br>MYSQL<br>MYSQL<br>BID<br>FRSIRT<br>SECUNIA<br>SECTRACK<br>XF |
| Niels Provos -- Honeyd | Unspecified vulnerability in Niels Provos Honeyd before 1.5b allows remote attackers to cause a denial of service (application crash) via certain Address Resolution Protocol (ARP) packets. | unknown<br>2006-08-22 | 2.3 | CVE-2006-4292<br>OTHER-REF<br>FRSIRT<br>SECUNIA<br>XF |

| | | | | |
|---|---|---|---|---|
| osCommerce -- osCommerce | Multiple directory traversal vulnerabilities in cache.php in osCommerce 2.2 Milestone 2 060817 allow remote attackers to determine existence of arbitrary files and disclose the installation path via a .. (dot dot) in unspecified parameters in the (1) tep_cache_also_purchased, (2) tep_cache_manufacturers_box, and (3) tep_cache_categories_box functions. | unknown<br>2006-08-22 | 2.3 | CVE-2006-4298<br>OTHER-REF<br>XF |
| Panda -- Panda ActiveScan | Cross-site scripting (XSS) vulnerability in ascan_6.asp in Panda ActiveScan 5.53.00 allows remote attackers to inject arbitrary web script or HTML via the email parameter. | 2006-01-08<br>2006-08-22 | 2.3 | CVE-2006-4295<br>OTHER-REF<br>BID<br>SECTRACK |
| Sony -- VAIO Media Server | Directory traversal vulnerability in Sony VAIO Media Server 2.x, 3.x, 4.x, and 5.x before 20060626 allows remote attackers to gain sensitive information via unspecified vectors. | unknown<br>2006-08-22 | 2.3 | CVE-2006-4290<br>OTHER-REF<br>OTHER-REF<br>BID<br>FRSIRT<br>SECUNIA<br>XF |
| Sun -- Java Web Start<br>Sun -- J2SE | The Java Plug-in J2SE 1.3.0_02 through 5.0 Update 5, and Java Web Start 1.0 through 1.2 and J2SE 1.4.2 through 5.0 Update 5, allows remote attackers to exploit vulnerabilities by specifying a JRE version that contain vulnerabilities. | unknown<br>2006-08-22 | 2.3 | CVE-2006-4302<br>SUNALERT<br>SECUNIA<br>SECTRACK<br>SECTRACK |
| Sun -- Solaris | Race condition in (1) libnsl and (2) TLI/XTI API routines in Sun Solaris 10 allows remote attackers to cause a denial of service ("tight loop" and CPU consumption for listener applications) via unknown vectors related to TCP fusion (do_tcp_fusion). | unknown<br>2006-08-22 | 1.9 | CVE-2006-4303<br>SUNALERT<br>SECTRACK<br>XF |
| Sun -- Java System Content Delivery Server | Unspecified vulnerability in Sun Java System Content Delivery Server 4.0, 4.1, and 5.0 allows local and remote attackers to read data from arbitrary files via unspecified vectors. | unknown<br>2006-08-25 | 2.3 | CVE-2006-4353<br>SUNALERT |
| Symantec -- Norton Personal Firewall | Symantec Norton Personal Firewall 2006 9.1.0.33, and possibly earlier, does not properly protect Norton registry keys, which allows local users to provide Trojan horse libraries to Norton by using RegSaveKey and RegRestoreKey to modify HKLM\SOFTWARE\Symantec\CCPD\SuiteOwners, as demonstrated using NISProd.dll. NOTE: in most cases, this attack would not cross privilege boundaries, because modifying the SuiteOwners key requires administrative privileges. However, this issue is a vulnerability because the product's functionality is intended to protect against privileged actions such as this. | unknown<br>2006-08-21 | 3.3 | CVE-2006-4266<br>BUGTRAQ<br>OTHER-REF<br>BID |
| Symantec -- Symantec Enterprise Security Manager | The manager server in Symantec Enterprise Security Manager (ESM) 6 and 6.5.x allows remote attackers to cause a denial of service (hang) via a malformed ESM agent request. | unknown<br>2006-08-23 | 2.3 | CVE-2006-4314<br>BUGTRAQ<br>OTHER-REF<br>BID<br>BID<br>FRSIRT<br>SECTRACK<br>SECUNIA |
| TikiWiki Project -- TikiWiki | Cross-site scripting (XSS) vulnerability in tiki-searchindex.php in TikiWiki 1.9.4 allows remote attackers to inject arbitrary web script or HTML via the highlight parameter. NOTE: the provenance of this information is unknown; the details are obtained from third party information. | unknown<br>2006-08-22 | 2.3 | CVE-2006-4299<br>BID<br>OSVDB<br>SECUNIA |
| VWar -- Virtual War | Cross-site scripting (XSS) vulnerability in calendar.php in Virtual War (VWar) 1.5.0 and earlier allows remote attackers to inject arbitrary web script or HTML via the year parameter. NOTE: The page parameter vector is covered by CVE-2006-4009. | unknown<br>2006-08-18 | 2.3 | CVE-2006-4224<br>BUGTRAQ |
| Wireshark -- Wireshark | Unspecified vulnerability in the SCSI dissector in Wireshark (formerly Ethereal) 0.99.2 allows remote attackers to cause a denial of service (crash) via unspecified vectors. | unknown<br>2006-08-24 | 2.3 | CVE-2006-4330<br>OTHER-REF<br>BID<br>FRSIRT<br>SECTRACK<br>SECUNIA |
| Wireshark -- Wireshark | Multiple off-by-one errors in the IPSec ESP preference parser in Wireshark (formerly Ethereal) 0.99.2 allow remote attackers to cause a denial of service (crash) via unspecified vectors. | unknown<br>2006-08-24 | 2.3 | CVE-2006-4331<br>OTHER-REF<br>BID<br>FRSIRT<br>SECTRACK<br>SECUNIA |
| Wireshark -- Wireshark | Unspecified vulnerability in the DHCP dissector in Wireshark (formerly Ethereal) 0.10.13 through 0.99.2, when run on Windows, allows remote attackers to cause a denial of service (crash) via unspecified vectors that trigger a bug in Glib. | unknown<br>2006-08-24 | 2.3 | CVE-2006-4332<br>OTHER-REF<br>BID<br>FRSIRT<br>SECTRACK |

| | | | | |
|---|---|---|---|---|
| | | | | SECUNIA |
| Wireshark -- Wireshark | The SSCOP dissector in Wireshark (formerly Ethereal) before 0.99.3 allows remote attackers to cause a denial of service (resource consumption) via malformed packets that cause the Q.2391 dissector to use excessive memory. | unknown<br>2006-08-24 | 2.3 | CVE-2006-4333<br>OTHER-REF<br>BID<br>FRSIRT<br>SECTRACK<br>SECUNIA |

Back to top

**Last updated August 28, 2006**